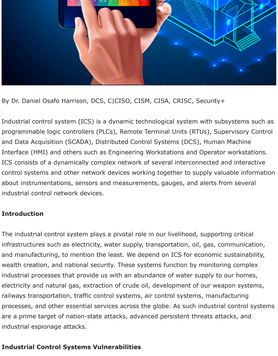
Industrial Control System Vulnerabilities: A Prime Target of Our Critical Infrastructure by Adversaries

By **News Team** - February 26, 2020



By Dr. Daniel Osafo Harrison, DCS, CICISO, CISM, CISA, CRISC, Security+

Industrial control system (ICS) is a dynamic technological system with subsystems such as programmable logic controllers (PLCs), Remote Terminal Units (RTUs), Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Human Machine Interface (HMI) and others such as Engineering Workstations and Operator workstations. ICS consists of a dynamically complex network of several interconnected and interactive control systems and other network devices working together to supply valuable information about instrumentations, sensors and measurements, gauges, and alerts from several industrial control network devices.

Introduction

The industrial control system plays a pivotal role in our livelihood, supporting critical infrastructures such as electricity, water supply, transportation, oil, gas, communication, and manufacturing, to mention the least. We depend on ICS for economic sustainability, wealth creation, and national security. These systems function by monitoring complex industrial processes that provide us with an abundance of water supply to our homes, electricity and natural gas, extraction of crude oil, development of our weapon systems, railways transportation, traffic control systems, air control systems, manufacturing processes, and other essential services across the globe. As such industrial control systems are a prime target of nation-state attacks, advanced persistent threats attacks, and industrial espionage attacks.

Industrial Control Systems Vulnerabilities

The demand for an Industrial Control System uptime compounded by the fact that most of the Industrial Control Systems are a legacy system that is near their end of life and have a limited integrated microprocessors chips, low system memories and uses an outdated operating system which often lacks the support for vendor's patch updates. Unfortunately, Fieldbus protocols that connect devices such as PLCs and Sensors have little to no security, backend protocols that enable systems to systems communication are also ridden with vulnerabilities. This phenomenon is a weakness that can be exploited by a determined attacker. In fact, in today's world, most of these systems are connected to the internet, which also increases the attack surface and present uber threat to ICS network (Paganini, 2013).

Suffice it to say, ICS premier support to our infrastructure, economy, and well-being makes them a target by industrial espionage aimed at stealing proprietary information or a nation-state attack like the Stuxnet and Night Dragon attacks to disrupt operations. Imagine the entire state of New York without electricity for a few days or the City of Chicago without water supply, think about the impact on society and businesses. I hope you get the picture!

Furthermore, the constant demand for the availability of the system also means we limit security protection because extreme cybersecurity safeguards such as intrusion prevention system (IPS) and packet inspection technologies can put enormous burden on these systems and networks which can completely depredate the network into a grinding halt (Stopping plant operations) as such the vulnerabilities outline below:

Lack of Patching and hardware failures:

Most ICS systems run on Windows XP operating system with zero patch releases available, which makes them susceptible to all forms of Trojan and Worms attacks. Additionally, hardware failure and inability to obtain replacement parts for these systems are common problems for end of life system. It cost vendors more money to support the end of life products. Vendors are forward thinkers and would rather invest their money on the most current and future products for profit maximization instead.

Lack of encryption:

The absence of encryption on the ICS network or devices means that all activities or transactions performed on the network are in a plain text format, which makes it susceptible to all forms of cyber-attacks. Encryptions convert plain text into a cipher-text that prevents unauthorized disclosure of sensitive information such as proprietary information, user identity and passwords, SQL transactions, protocol communications, setpoints, gauges, and so forth. Encryption protects confidentiality by keeping sensitive information private. Digital signatures used to encrypt the sender's private key to validate the integrity of information from the sender (Systems) and none-repudiation. This way, the sender is unable to deny sending sensitive information across a network to another device. However, encryption is known to create several issues on the ICS network; hence due care and due diligence must be considered before deploying encryption.

Human Error:

Systems misconfiguration and inadequate firewall rules can create a huge vulnerability that can be exploited by adversaries. All it takes is for a well-intended automation engineer or cognizant engineer to unknowingly insert malware-infected USB into a workstation or a server to cause havoc on the network. Once upon a time, an automation engineer forgot to properly save a configuration changes he made to a cisco 2960 switches because he failed to "copy running-configuration and startup-configuration." Running-config is volatile, and startup-config is nonvolatile RAM (NVRAM), his actions created a self-inflicted denial of service disrupting production. Imagine how much productivity and money lost.

Inadequate Access Control Management:

Often, ICS systems require little to no identification, authentication, and authorization process to restrict user access, and this action presents a vulnerability that can be exploited by both external attackers and disgruntle insider. A successful attacker may gain full access to critical systems on the network, thereby disrupting production operations.

Mitigating ICS Vulnerabilities

According to the NIST SP 800-82 Revision 2 publication, the following steps can mitigate a lot of the vulnerabilities associated with ICS networks and systems.

- Employ application whitelisting to protect infrastructure from potentially harmful programming. For instance, PLCs don't need Microsoft office install on them.
- Implement configuration management and patch management controls to keep control systems secure. Establishing a Security Configuration Management Board that reviews all system configuration and approve them before deployment to production will mitigate risks.
- Reduce attack surface areas by segmenting networks into logical parts by functional groups such as cognizant engineering, automation engineering, control room operators, historian, business network, and so forth and restricting host-to-host communications paths.
- Require multi-factor authentication and enforce the principle of least privilege (POLP) wherever possible, use expert judgment.
- Require remote access to be operator controlled and time-limited.
- Monitor traffic within the control network and on ICS perimeters (enclave). For example, deploying Security Information and Event Management (SIEM) for continuous monitoring will help identify issues on the network as well monitor implemented security controls
- Analyze access logs and verify all anomalies.
- Employ a robust back and recovery program for the ICS network.

Conclusion

In a nutshell, the ICS network is vulnerable and attractive to APT, Nation-State, and other forms of attacks that aim at stealing sensitive information and proprietary information. There are many issues to take into consideration when creating a risk assessment for the industrial control systems. The organization must first analyze what they are going to look for and then evaluate the process. Stakeholders should be part of the internal evaluation process because the people within an organization understand their organization the best. Conduct assessments using regulations from the local, state, or federal programs/standards, and implement security controls to reduce risks on the ICS network to a level the organization is willing to accept.

References

Pierluigi Paganini (2013, Dec). Two Million Social Media Credentials Stolen by Cybercriminals. Retrieved from http://securityaffairs.co/wordpress/20219/cyber-crime/two-million-credentials-stolen.html

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security. (2015) NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

About the Author

Dr. Daniel Osafo Harrison, DCS, CICISO, CISM, CISA, CRISC, Security+

Dr. Harrison is a Doctor of Computer Science in Information Assurance and Head of Cybersecurity. Background in Industrial Control System Cybersecurity, DoD Information Assurance, Artificial Intelligence, Enterprise Network Architecture Security, Computer Programming, and Laboratory Information Systems. Contact me at daniel@docharrison.org, and https://www.linkedin.com/in/dr-daniel-harrison-dcs-ciso-ciscism-sec-38459015/

TAGS: Account Adware Apple Bitcoin botnet Cyber Security Iot Irish it security Magazine network Russia russian Security software VPN vulnerability

Previous article
Cross Domain Solutions – Quo Vadis

Next article
The Secret to Winning IT Security Roulette

News Team
https://www.cyberdefensemagazine.com

RELATED ARTICLES MORE FROM AUTHOR

News
Automated Pentesting – Ready to Replace Humans?

News
Zero Trust Model Is Meaningless Without TLS Inspection

News
Emotet Attacks Surge in 2020, but Could Be Prevented